



# CVE-2019-3846

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2019-3846
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-06-03 19:29:00 UTC
<b>Updated</b>	2023-02-12 23:38:00 UTC
<b>Description</b>	A flaw that allowed an attacker to corrupt memory and possibly escalate privileges was found in the mwifiex kernel module

## Risk And Classification

**Problem Types:** CWE-122

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All

Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	-	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">A700s</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">A700s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">A700s Firmware</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">A700s Firmware</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Unified Manager For Vmware Vsphere</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Unified Manager For Vmware Vsphere</a>	All	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Cn1610</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Cn1610</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Cn1610 Firmware</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Cn1610 Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H610s</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H610s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H610s Firmware</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H610s Firmware</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Hci Management Node</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Hci Management Node</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Solidfire</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Solidfire</a>	-	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All

## References

### Reference

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Red Hat Customer Portal
Bugtraq: [slackware-security] Slackware 14.2 kernel (SSA:2019-202-01)
Red Hat Customer Portal
Bugtraq: [SECURITY] [DSA 4465-1] linux security update
[security-announce] openSUSE-SU-2019:1570-1: important: Security update
1713059 – (CVE-2019-3846) CVE-2019-3846 kernel: Heap overflow in mwifiex_update_bss_desc_with_ie function in marvell/mwifiex/scan.c
Red Hat Customer Portal - Access to 24x7 support and knowledge
Red Hat Customer Portal
Debian -- Security Information -- DSA-4465-1 linux
USN-4095-2: Linux kernel (Xenial HWE) vulnerabilities   Ubuntu security notices   Ubuntu
Red Hat Customer Portal
Red Hat Customer Portal
USN-4095-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu
June 2019 Linux Kernel Vulnerabilities in NetApp Products   NetApp Product Security
USN-4118-1: Linux kernel (AWS) vulnerabilities   Ubuntu security notices   Ubuntu
[SECURITY] [DLA 1823-1] linux security update
USN-4117-1: Linux kernel (AWS) vulnerabilities   Ubuntu security notices   Ubuntu
[SECURITY] Fedora 30 Update: kernel-headers-5.1.7-300.fc30 - package-announce - Fedora Mailing-Lists
Red Hat Customer Portal
USN-4094-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu
[SECURITY] Fedora 29 Update: kernel-headers-5.1.6-200.fc29 - package-announce - Fedora Mailing-Lists
Red Hat Customer Portal
USN-4093-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu
[SECURITY] Fedora 29 Update: kernel-headers-5.1.6-200.fc29 - package-announce - Fedora Mailing-Lists
Kernel Live Patch Security Notice LSN-0058-1 ≈ Packet Storm
1713059 – (CVE-2019-3846) CVE-2019-3846 kernel: Heap overflow in mwifiex_update_bss_desc_with_ie function in marvell/mwifiex/scan.c
[SECURITY] [DLA 1824-1] linux-4.9 security update
Slackware Security Advisory - Slackware 14.2 kernel Updates ≈ Packet Storm
[security-announce] openSUSE-SU-2019:1579-1: important: Security update
[security-announce] openSUSE-SU-2019:1571-1: important: Security update
Kernel Live Patch Security Notice LSN-0054-1 ≈ Packet Storm
[SECURITY] Fedora 30 Update: kernel-headers-5.1.7-300.fc30 - package-announce - Fedora Mailing-Lists
oss-sec: CVE-2019-3846 : Marvell Wifi Driver mwifiex mwifiex_update_bss_desc_with_ie Heap Overflow
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

375413 IBM Security Guardium kernel Vulnerability (6152439)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**